VŠB – Technická univerzita Ostrava
Fakulta strojní
Institut dopravy

Použití principů funkční bezpečnosti u kolejových vozidel

Using of Functional Safety for Rail Vehicles

Student: František Rýznar
Vedoucí bakalářské práce: Ing. Jan Famfulík, Ph.D.

Ostrava 2010

VŠB - Technická univerzita Ostrava
Fakulta strojní
Institut dopravy

Zadání bakalářské práce

Student: **František Rýznar**

Studijní program: B2341 Strojírenství

Studijní obor: 2301R002 Dopravní technika

Téma: Použití principů funkční bezpečnosti u kolejových vozidel
Using of Functional Safety for Rail Vehicles

Zásady pro vypracování:

Cíl:
Vypracovat analýzu funkční bezpečnosti teplovodního topení vybraného motorového vozu.

Osnova:
1. Principy a zásady hodnocení funkční bezpečnosti dle ČSN EN 61508
2. Technický popis vybraného typu teplovodního topení
3. Analýza rizik teplovodního topení dle metodiky ČSN EN 61508
4. Technické a ekonomické hodnocení výsledků analýzy rizik

Seznam doporučené odborné literatury:

Norma ČSN EN 61508
Podklady výrobce teplovodního topení
Famfulík, J. Teorie údržby. VŠB – TU Ostrava, 2006. ISBN 80-248-1029-8

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Jan Famfulík, Ph.D.**

Datum zadání: 18.12.2009
Datum odevzdání: 21.05.2010

doc. Ing. Vladimír Smrž, Ph.D.
vedoucí katedry

prof. Ing. Radim Farana, CSc.
děkan fakulty

Místopřísežné prohlášení studenta

Prohlašuji, že jsem celou bakalářskou práci včetně příloh vypracoval samostatně pod vedením vedoucího bakalářské práce a uvedl jsem všechny použité poklady a literaturu.

V Ostravě: 17.5.2010 …..……

podpis studenta

Prohlašuji, že

- jsem byl seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo.

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen „VŠB-TUO“) má právo nevýdělečně ke své vnitřní potřebě bakalářskou práci užít (§ 35 odst. 3).

- souhlasím s tím, že bakalářská práce bude v elektronické podobě uložena v Ústřední knihovně VŠB-TUO k nahlédnutí a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o kvalifikační práci, obsažené v Záznamu o závěrečné práci, umístěném v příloze mé kvalifikační práce, budou zveřejněny v informačním systému VŠB-TUO.

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona.

- bylo sjednáno, že užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

- beru na vědomí, že odevzdáním své práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, bez ohledu na výsledek její obhajoby.

V Ostravě: 17.5.2010

……..…….
podpis

Jméno a příjmení autora práce: František Rýznar

Adresa trvalého pobytu autora práce: Klubovní 245
789 69 Postřelmov

ANOTACE BAKALÁŘSKÉ PRÁCE

RÝZNAR, F. Použití principů funkční bezpečnosti u kolejových vozidel: bakalářská práce. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy, 2010, 44 s. Vedoucí práce: Famfulík, J.

Bakalářská práce se zabývá funkční bezpečností, hlavně analýzou rizika a stanovením úrovní integrity bezpečnosti (SIL). V úvodní části jsou uvedeny základní pojmy bezpečnosti, zásady hodnocení funkční bezpečnosti, popis metody analýzy rizika FMEA a metod pro určení úrovně integrity bezpečnosti SIL. Analýza rizika FMEA je aplikována na nezávislé teplovodní topení typu HYDRONIC L35 od výrobce Eberspächer. Přiřazení úrovní integrity bezpečnosti daným komponentům je provedeno pomocí metody diagramu rizika. Nakonec je zhodnocena redukce rizika možnosti vzniku poruchy bez opatření a s opatřeními.

ANNOTATION OF BACHELOR THESIS

RÝZNAR, F. Using of Functional Safety for Rail Vehicles: Bachelor Thesis. Ostrava: VŠB – Technical Univerzity of Ostrava, Faculty of Mechanical Engineering, Institute of Transporting, 2010, 44 s. Thesis head: Famfulík, J.

Bachelor thesis is dealing with functional safety, mainly risk analysis and set a safety integrity level (SIL). The introduction contains main concepts of safety, principles for evaluation of functional safety, description method of risk analysis FMEA and methods for set a safety integrity level (SIL). Risk analysis FMEA has been applied to Eberspächer Hydronic L35 Water Heater. Assignment of safety integrity level is made by method called diagram of risk. In the end risk reduction is valorised, it means possibility of failure origin without securing and with securing.

Obsah

Seznam použitých symbolů a značek

ALARP	Co nejnižší rozumně dosažitelné riziko
C	Následek nebezpečné události
ČSN	Česká státní norma
DIN	Německá národní norma (Deutsche Industrie-Norm)
E/E/PE	Elektrický/elektronický/programovatelný elektronický
EN	Evropská norma
EUC	Řízené zařízení
F	Výskyt a doba vystavení v nebezpečné oblasti
FMEA	Analýza způsobů a důsledků poruch (Failure Mode and Effect Analysis)
F_{np}	Četnost, s níž by se mohla nebezpečná událost vyskytovat bez použití jakýchkoliv ochranných prostředků
F_p	Četnosti rizika za přítomnosti ochranných prostředků
F_t	Četnost přípustného rizika
IP	Stupeň zabezpečení (International Protection)
KV	Kolejové vozidlo
LCD	Displej z tekutých krystalů (Liquid crystal display)
P	Možnost se nebezpečné události vyhnout
PFD_{avg}	Střední pravděpodobnost poruchy při vyžádání systému souvisejícího s bezpečností
RPN	Hodnota významnosti rizika (Risk Priority Number)
SIL	Safety Integrity Level (úroveň integrity bezpečnosti)
SV	Silniční vozidlo
W	Pravděpodobnost nežádoucího výskytu
ΔR	Nutné snížení rizika.

0 Úvod

Pojem funkční bezpečnosti představuje mezinárodně uznávaný bezpečnostní standard pro zařízení, kde jsou využívány E/E/PE systémy zaručující bezpečnost. Funkční bezpečností se zabývá norma ČSN EN 61508, která popisuje obecné zásady celkové bezpečnosti a tvoří základ bezpečnosti u jiných systémů. Tato norma je tedy obecným dokumentem určeným pro jednotlivá odvětví průmyslu. Náplň této práce byla čerpána především v uvedené normy.

Každé technické zařízení představuje pro své okolí určité riziko, které může mít za důsledek ohrožení zdraví lidí nebo ohrožení životního prostředí. A proto v současné době je pojem funkční bezpečnosti velmi aktuální a žádaný. Funkční bezpečnost se využívá tam, kde je příčinou nebezpečí selhání určité funkce systému. Systém využívající funkční bezpečnost vyhovuje mezinárodním normám týkající se bezpečnosti. Hlavním cílem funkční bezpečnosti je snížení rizika zranění osob, poškození životního prostředí nebo materiálových ztrát.

V dnešní době se funkční bezpečnost běžně aplikuje v elektrotechnice, energetice, protipožární ochraně, zábavních a sportovních zařízeních, dopravě, apod.

Tato práce obsahuje definice základních pojmů bezpečnosti, které jsou důležité pro hodnocení funkční bezpečnosti. Výsledkem analýzy rizika je stanovení úrovně integrity bezpečnosti, z tohoto důvodu jsou v práci uvedeny metody pro určení úrovně integrity bezpečnosti, a to jak kvantitativní, tak metody kvalitativní. Tyto metody jsou postaveny na principu ALARP, jehož stručný popis je také součástí této práce.

Dosažené poznatky o hodnocení funkční bezpečnosti jsou aplikovány na vybraný typ teplovodního topení značky Eberspächer, konkrétně se jedná o typ HYDRONIC L35. Tento typ teplovodního topení se nejčastěji využívá pro nezávislé topení u kolejových vozidel, například u motorových vozů Regionova. Součástí práce je také technický popis daného typu teplovodního topení.

Jako cíl práce bylo stanoveno zhotovit analýzu rizika na vybraném typu teplovodního topení. Ke komponentům, jejichž poruchou by mohlo dojít ohrožení života osob, přiřadit danou hodnotu úrovně integrity bezpečnosti. Výsledky této práce mohou být určeny pro zvýšení bezpečnosti zařízení vzhledem k okolí.

1 Základní pojmy bezpečnost dle ČSN EN 61508

V této kapitole je uvedena stručná definice pojmu funkční bezpečnost a dále definice nejzákladnějších pojmů z oblasti celkové bezpečnosti, které uvádí norma ČSN EN 61508.

1.1 Definice funkční bezpečnosti

Funkční bezpečnost je část celkové bezpečnosti, která je závislá na správném fungování systémů E/E/PE, které zajišťují její bezpečnost. Platí tedy pro EUC a systémy řízení EUC, kde E/E/PE jednotky plní bezpečnostní funkce. Hlavním cílem pro aplikaci funkční bezpečnosti je snížit riziko možnosti zranění lidí, narušení životního prostředí nebo možnost materiálových ztrát. [2]

1.2 Základní termíny bezpečnosti

Poškození (újma) – zranění nebo poškození zdraví lidí, ke kterému může dojít přímo, nebo nepřímo v případě, kdy dojde ke zhoršení nebo ztrátě určitých vlastností systému,

Nebezpečí – zdroj poškození pro osoby, ke kterému může dojít v časově krátké době (např. požár) nebo má dlouhodobý účinek na zdraví osob (např. uvolněná toxická látka),

Nebezpečná situace – situace, ve které je osoba vystavena nebezpečí,

Nebezpečná událost – situace, jejímž výsledkem je poškození,

Porucha – systém ztrácí schopnost vykonávat požadovanou funkci,

Bezpečná porucha – chyba, která nenaruší funkci systému nebo nezpůsobí nebezpečný stav systému,

Nebezpečná porucha – taková chyba, která uvede systém do nebezpečného stavu, kdy není schopen vykonávat požadovanou funkci,

Riziko – kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození,

Přípustné riziko – takové riziko, které je přijatelné v daných situacích,

Zbytkové riziko – takové riziko, které stále hrozí i po přijetí bezpečnostních opatření,

Bezpečnost – odstranění nepřijatelného rizika,

Primární bezpečnost – bezpečnost, která se přímo zaměřuje na nebezpečí zranění osob,

Nepřímá bezpečnost – zahrnuje takové důsledky poruchové funkce systému, které neohrožují zdraví osob,

Bezpečný stav – stav, kdy je dosaženo bezpečnosti ,

Vada – stav, který může způsobit snížení nebo ztrátu způsobilosti funkční jednotky plnit požadovanou funkci. [2]

2 Vyhodnocení funkční bezpečnosti dle ČSN EN 61508

Kapitola zabývající se analýzou nebezpečí a rizik. Jsou zde uvedeny základní pojmy, zásady analýzy rizika, popsána metoda analýzy způsobů a důsledků poruch FMEA a metody pro stanovení úrovní integrity bezpečnosti, které uvádí norma ČSN EN 61508.

2.1 Požadavky celkové bezpečnosti

a) pro každé nebezpečí je nutné určit bezpečnostní funkce sloužící pro zajištění požadované funkční bezpečnosti,
b) pro každou nebezpečnou událost se musí provést nutné snížení rizika (kvantitativním nebo kvalitativním způsobem),
c) pokud vyžadují poruchy systému řízení EUC zásah jednoho nebo několika E/E/PE systému souvisejících s bezpečností nebo systémů souvisejících s bezpečností pracujících na jiných technických principech, musí se použít následující požadavky:
   - intenzita nebezpečných poruch musí být prodloužena na základě dat získaných pomocí skutečných provozních zkušeností, na základě analýzy bezporuchovosti nebo z informací z průmyslové databáze bezporuchovosti,
   - intenzita nebezpečných poruch nesmí být nižší než 10^{-5}
   - při zpracovávání požadavků celkové bezpečnosti se musí zohlednit všechny předvídatelné režimy nebezpečných poruch
   - systém řízení EUC musí být nezávislý na E/E/PE systémem souvisejících s bezpečností,
d) pro každou bezpečnostní funkci je nutné stanovit požadavky integrity bezpečnosti z hlediska nutného snížení rizika,

e) specifikace požadavků celkové bezpečnosti musí být tvořena ze specifikace bezpečnostních funkcí a ze specifikace požadavků integrity bezpečnosti. [2]

2.2 Požadavky na určení nebezpečných událostí EUC a systému řízení EUC

a) analýza rizika se může provádět i více než jednou na stejném zařízení. To je nutné tehdy, když v průběhu životního cyklu celkové bezpečnosti dojde k změně základu, na kterém byla předchozí rozhodnutí stanovena,
b) při určování nebezpečných událostí je nutné zohlednit všechny rozumně předvídatelné okolnosti (tzn. nejen poruchových podmínek zařízení, ale i nebezpečí, které může vzniknout při nesprávném použití daného zařízení vlivem chyby lidského faktoru). Je tedy nutné určit sled událostí, které vedou k nebezpečnému stavu, stanovit pravděpodobnost jednotlivých nebezpečných událostí a určit důsledky spojené s nebezpečnými událostmi,
c) pro každou takto stanovenou nebezpečnou událost je nutné vyhodnotit a stanovit riziko,
d) analýza rizika se stanoví pomocí kvantitativních nebo kvalitativních technik. [2]

2.3 Riziko a integrita bezpečnosti

Základní pojmy:

Riziko:

- kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození,

Nutné snížení rizika:

- takové snížení rizika, aby bylo zajištěno nepřekročení přípustného rizika,
- má být dosaženo pomocí E/E/PE systémů souvisejících s bezpečností a systémů souvisejících s bezpečností, které pracují na jiných technických principech,

Integrita bezpečnosti:

- je definována jako pravděpodobnost systému plnit jeho bezpečnostní funkce po stanovenou dobu a za všech stanovených podmínek. [2]

2.3.1 Analýza rizika

Analýza rizika je nedílnou součástí bezpečnostního cyklu. Umožňuje určit nebezpečné situace a bezpečnostní funkce pro požadovanou integritu bezpečnosti. Představuje jeden za základních konceptů při zpracování funkční bezpečnosti. Stanovena tak, že pokrývá všechny činnosti životního cyklu celkové bezpečnosti, kterými jsou:

a) počáteční koncept,
b) definice celkového předmětu,
c) analýza nebezpečí a rizika,
d) stanovení bezpečnostních požadavků,
e) specifikace,
f) návrh,
g) provoz a údržba,
h) modifikace,
i) předání do provozu nebo vyřazení z provozu.

Pro použití analýzy rizik je nutné nejdříve specifikovat zařízení, na kterém budeme analýzu provádět. To platí i pro EUC a systémy řízení EUC. Dále se určí typ události, která může vyvolat nehodu. Další krok je snížení rizika. A jako poslední krok je nutné, informace a dosažené výsledky zdokumentovat.

Analýza rizika musí zvážit:

- každou událost, která vede k nebezpečí,
- okolnosti, se kterými je každá nebezpečná událost spojena,
- pravděpodobnost sledu událostí vedoucích k nebezpečné události,
- snížení rizika pro každou nebezpečnou událost,
- provést opatření pro snížení nebo odstranění nebezpečí a rizik,
- předpoklady stanovené během analýzy rizik se musí podrobně popsat. [2]

2.3.2 Integrita bezpečnosti

Integrita bezpečnost je pravděpodobnost systému souvisejícího s bezpečností plnit požadované funkce po stanovenou dobu a za stanovených podmínek. Integrita bezpečnosti se týká takových vlastností systému, u kterých je bezpečné provádět bezpečnostní funkce. Čím vyšší je úroveň integrity bezpečnosti u systémů souvisejících z bezpečností, tím menší je pravděpodobnost selhání těchto systémů. Norma ČSN EN 61508 rozděluje integritu bezpečnosti do čtyř úrovní.

Při určování úrovně integrity bezpečnosti je nutné zohlednit všechny příčiny poruch (náhodné i systematické), které vedou k nebezpečnému stavu. Prvky, které tvoří integritu bezpečnosti jsou – integrita bezpečnosti softwaru, integrita bezpečnosti hardwaru a systematická integrita bezpečnosti:

1) **integrita bezpečnosti softwaru** – pravděpodobnost, že software v elektronickém programovatelném systému plní požadované bezpečnostní funkce,
2) **integrita bezpečnosti hardwaru** – patří do integrity týkající se bezpečnosti systémů souvisejících s bezpečností a týká se náhodných poruch hardwaru v režimu poruchy,
3) **systematická integrita bezpečnosti** – patří do integrity týkající se bezpečnosti systémů souvisejících s bezpečností a týká se systematických poruch v režimu nebezpečných poruch.

Požadovaná integrita bezpečnosti, pro snížení rizika, musí mít takovou úroveň, aby zajistila, že četnost nebezpečných poruch nepřekročila požadovanou hodnotu a aby četnost poruch byla dostatečně malá. [2]

2.3.3 Úroveň integrity bezpečnosti SIL (Safety Integrity Level)

Norma ČSN EN 61508 rozděluje integritu bezpečnosti do čtyř úrovní. Nejvyšší úroveň integrity u systémů týkajících se bezpečnosti je 4, nejnižší úroveň je 1.

a) **režim s nízkým vyžádáním** – četnost vyžádání provozu systému souvisejícího s bezpečností není vetší než jednou ročně nebo není větší než dvojnásobek četnosti periodických zkoušek,
b) **režim s vysokým vyžádáním** – četnost vyžádání provozu systému souvisejícího s bezpečností je vetší než jednou ročně nebo je větší než dvojnásobek četnosti periodických prohlídek. [2]

Tabulka č.1 – Úrovně integrity bezpečnosti: Pro režim s nízkým vyžádáním [2]

Úroveň integrity bezpečnosti	**Pravděpodobnost poruchy při vyžádání ochranného systému souvisejícího s bezpečností**
4	$\geq 10^{-5}$ až $< 10^{-4}$
3	$\geq 10^{-4}$ až $< 10^{-3}$
2	$\geq 10^{-3}$ až $< 10^{-2}$
1	$\geq 10^{-2}$ až 10^{-1}

Tabulka č.2 – Úrovně integrity bezpečnosti: Pro režim s vysokým vyžádáním [2]

Úroveň integrity bezpečnosti	**pravděpodobnost nebezpečných poruch [h^{-1}]**
4	$\geq 10^{-9}$ až $< 10^{-8}$
3	$\geq 10^{-8}$ až $< 10^{-7}$
2	$\geq 10^{-7}$ až $< 10^{-6}$
1	$\geq 10^{-6}$ až 10^{-5}

2.4 Analýza způsobů a důsledků poruch FMEA

Jedná se o kvalitativní metodu hodnocení funkční bezpečnosti. Slouží k analýze bezpečnosti a bezporuchovosti zařízení. Výsledkem analýzy FMEA je určení hodnoty významnosti rizika, tzv. RPN a zanesení nejvážnějších důsledků poruch, daného komponentu, do matice závažnosti. Všeobecně platí, že čím vyšší RPN tím je důsledek daného rizika závažnější. [1]

2.4.1 RPN (Risk Priority Number)

$$RPN = závažnost * četnost * odhalitelnost [-] \quad [1]$$

Klasifikace ukazatelů RPN

a) Závažnost poruchy:

Závažnost poruchy je známka (1-10) přiřazená nejzávažnějšímu důsledku poruchy. Při klasifikaci závažnosti poruchy je tedy nutné si jednotlivá rizika zařadit do jednotlivých stupňů podle toho, jak závažný důsledek může dané riziko způsobit. Proto je nutné sestavit tabulku, ve které se přesně stanoví závažnosti jednotlivých poruch. Ukázka tabulky závažnosti poruchy viz. tabulka č.3. [1]

Tabulka č.3 – Klasifikace závažnosti poruchy [1]

Závažnost poruchy		**Popis poruchy**
1	Žádný důsledek	Nemá vliv na funkce zařízení
2	Nepatrný důsledek	Nezásadní porucha
…….		
10	Velmi nebezpečný důsledek	Neočekávaná poruchy ohrožující bezpečnost

b) Určení četnosti poruchy:

Jedná se o stanovení četnosti s jakou je možné, že se daná porucha bude vyskytovat. Četnosti jednotlivých poruch opět rozdělujeme do několika stupňů (zpravidla 10), které přesně klasifikují jednotlivé četnosti. Četnost může být určena pomocí zkušeností s jednotlivými komponenty, nebo podle toho jestli se jedná o elektronickou součást nebo součást mechanickou. Dále ji můžeme například určit pomocí informace, v jakém prostředí dané komponenty pracují (teplotně namáhané, vystaveny vibracím, apod.). [1]

Tabulka č.4 – Klasifikace četnosti poruchy [1]

Četnost poruchy	
1	Téměř nikdy
2	Slabá
……	
10	Téměř jistá

c) Odhalitelnost poruchy:

Určení stupně možnosti odhalit případnou poruchu na základě vnějších prostředků (např. osoba obsluhující dané zařízení).

Tabulka č.5 – Klasifikace odhalitelnosti poruchy [1]

Odhalitelnost poruchy	
1	Téměř jistá
2	vysoká
……	
10	Téměř nemožná

d) Po přiřazení jednotlivých známek k danému riziku jsme schopni stanovit hodnotu RPN.

2.4.2 Matice závažnosti (kritičnosti)

Hodnota významnosti rizika **RPN** (Risk Priority Number) [-]						
	500					Čidlo plamene (chyba funkce)
	400					
	300			Elektromotor (chyba funkce)		
	200			Netěsnost tepelného výměníku Magnetický ventil (chyba funkce)		
	100	Překročení horní napěťové hranice Překročení dolní napěťové hranice	Nefunkčnost zdroje elektrické energie Netěsnost přívodního vedení chladící kapaliny	Čidlo teploty (chyba funkce) Zanesený palivový filtr Čidlo přehřívání (chyba funkce) Generátor zapalovací jiskry (chyba funkce)		
	0	nevýznamná 1,2	nezávažná 3,4	závažná 5,6	kritická 7,8	katastrofická 9,10
						Závažnost poruchy [-]

Obr. 1 – matice závažnosti

Jedná se o graf závislosti hodnoty RPN na závažnosti poruchy, kterou rozdělujeme do několika skupin. Závažnost poruchy určujeme pomocí přiřazené známky při klasifikaci rizika. Pomocí matice závažnosti jsme schopni určit jakým komponentům bude nutné přiřadit bezpečnostní funkce. Ukázka matice závažnosti je uvedena na obrázku č.1. Vyplněná matice je rozdělena do několika skupin (zpravidla 3), které jsou barevně odlišeny. Tyto skupiny nám rozdělují rizika do různých stupňů. Jednotlivé stupně jsou podrobněji popsány v kapitole 2.5. Pro vyplněnou matici závažnosti tedy platí, že pro komponenty nacházející se v červeném poli je nutné snížení rizika, pro komponenty ve žlutém poli je možné snížení rizika a pro komponenty v zeleném poli není nutné provést snížení rizika. Snížení rizika se provádí pomocí koncepce ALARP, která je podrobněji popsána v kapitole 2.5.

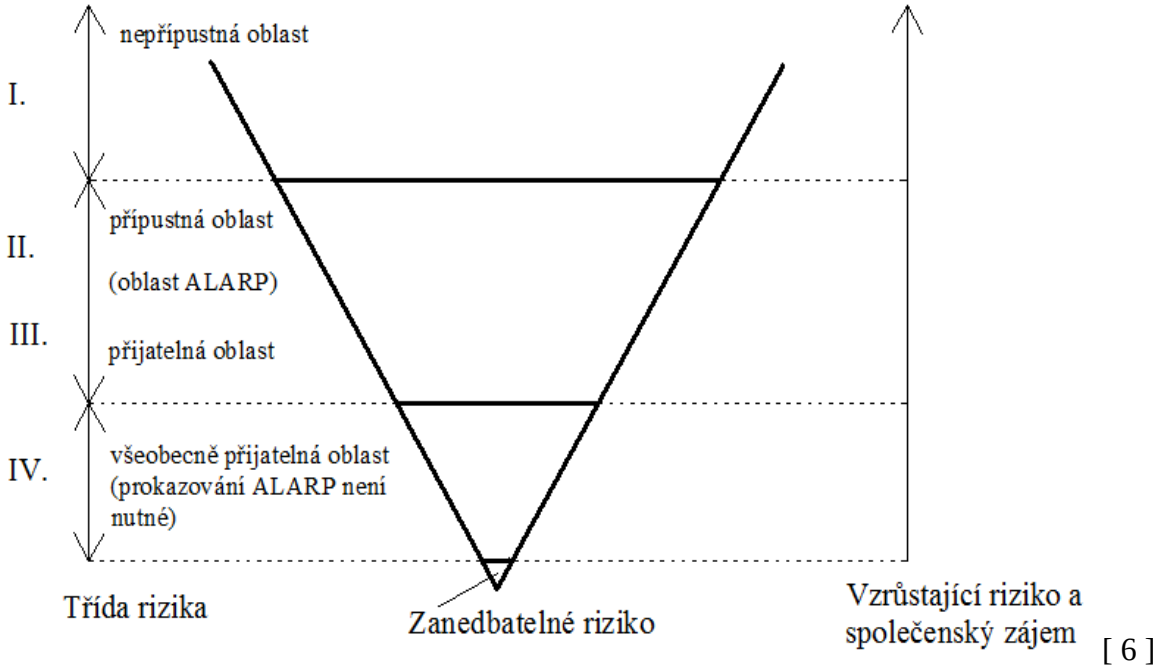
2.5 Koncepce ALARP

Koncepce ALARP umožňuje k hodnocení rizika využít kvantitativních i kvalitativních metod. Pro dosažení přípustného rizika pomocí principu ALARP, je nutné nejdříve uvést rozdělení rizik do tří různých stupňů:

a) riziko je příliš velké, proto je považováno za nepřípustné, a tak je nutné jej zcela odmítnout (vyloučit),
b) riziko je příliš malé (nebo už předtím bylo sníženo), že jeho působení bude bezvýznamné. V této oblasti není nutné žádné jednotlivé činnosti prokazovat pomocí ALARP, ale je nezbytné věnovat pozornost tomu, aby se dané (bezvýznamné) riziko udrželo na této úrovni,
c) riziko se nachází mezi stavy a) a b), a bylo již sníženo na přípustnou úroveň se zvážením z hlediska přínosů a z hlediska nákladů spojených s jeho dalším snižováním.

[2]

Nachází-li se riziko na úrovni a) je nutné ho pomocí principu ALARP snížit na co nejnižší rozumně možnou úroveň nebo na nejnižší rozumně proveditelnou úroveň. Tzn. musí být sníženo tak, aby se dostalo do přípustné (přijatelné) nebo do všeobecně přijatelné oblasti. Nebo nebezpečí způsobující riziko musí být odstraněno. Pokud se poté, co byl použit princip ALARP, riziko nachází mezi stupni a) a b), potom je toto riziko považováno za přípustné.
Tato metoda je nazývána jako třípásmová a je graficky znázorněna na obrázku č.2. [6]



[6]

Obr. 2 – Třípásmová metoda (model ALARP)

2.5.1 Cíl přípustného rizika

Jeden ze způsobů, kterým lze dosáhnout přípustného rizika, je stanovení počtu následků, ke kterým se přiřadí jednotlivé přípustné četnosti. Říkáme tomu slaďování následků. Toto slaďování následků by mělo být prováděno formou diskuse mezi jednotlivými zainteresovanými stranami. Při zohlednění koncepce ALARP může být slaďování následků provedeno formou tříd rizika. Jednotlivé třídy jsou vyznačeny na obrázku č.2 a jejich význam je uveden v tabulce č.6. [2]

Tabulka č.6 – Výklad jednotlivých tříd rizika dle ČSN EN 61508 [2]

Třída rizika	Výklad
Třída I	Nepřípustné riziko
Třída II	Nežádoucí riziko, přípustné pouze v případě, že je neproveditelné snížení rizika nebo, že náklady jsou neúměrné dosažitelnému zlepšení
Třída III	Přípustné riziko tehdy, když by náklady na snížení rizika přesáhly dosažené zlepšení
Třída IV	Zanedbatelné riziko

Tabulka č.7 – Klasifikace rizika (ukázkový příklad) [2]

Četnost	**Následek**			
	Katastrofální	**Kritický**	**Nepodstatný**	**Zanedbatelný**
Častá	I	I	I	II
Pravděpodobná	I	I	II	III
Příležitostná	I	II	III	III
Málo častá	II	III	III	IV
Nepravděpodobná	III	III	IV	IV
Neuvěřitelná	IV	IV	IV	IV
Pomocí četností uvedených v této tabulce určujeme úrovně integrity bezpečnosti pomocí kvantitativní metody.				

2.6 Metody určení úrovní integrity bezpečnosti

Vhodnost uvedených metod i rozsah jejich použití závisí na:

a) požadavcích vyplývajících ze zákonných a bezpečnostních předpisů,
b) konkrétních nebezpečích,
c) následcích vyplývajících z daného nebezpečí,
d) oblasti, pro kterou jsou aplikovány,
e) riziku EUC,
f) přesných datech, na kterých bude analýza založena. [2]

2.6.1 Metoda kvantitativní

Metoda kvantitativní se používá v případě, kdy:

- se přípustné riziko stanovuje pomocí číselného vyjádření (např. četnost poruch by neměla být vetší než jednou za 10^4 roků)
- už jsou stanoveny číselné hodnoty úrovní integrity bezpečnosti systémů souvisejících s bezpečností viz. tabulky č.1 a 2.

Hlavní kroky u této metody jsou:

- určení přípustného rizika (např. tabulka č.7),
- určení rizika EUC – skládá se z F_{np} a následku nebezpečné události,
- určení nutného snížení rizika a dosažení přípustného rizika.

Hlavní kroky této metody je třeba provést u každé bezpečnostní funkce, kterou má systém související s bezpečností realizovat.

Definice proměnných:

PFD_{avg} – střední pravděpodobnost poruchy při vyžádání systému souvisejícího s bezpečností,

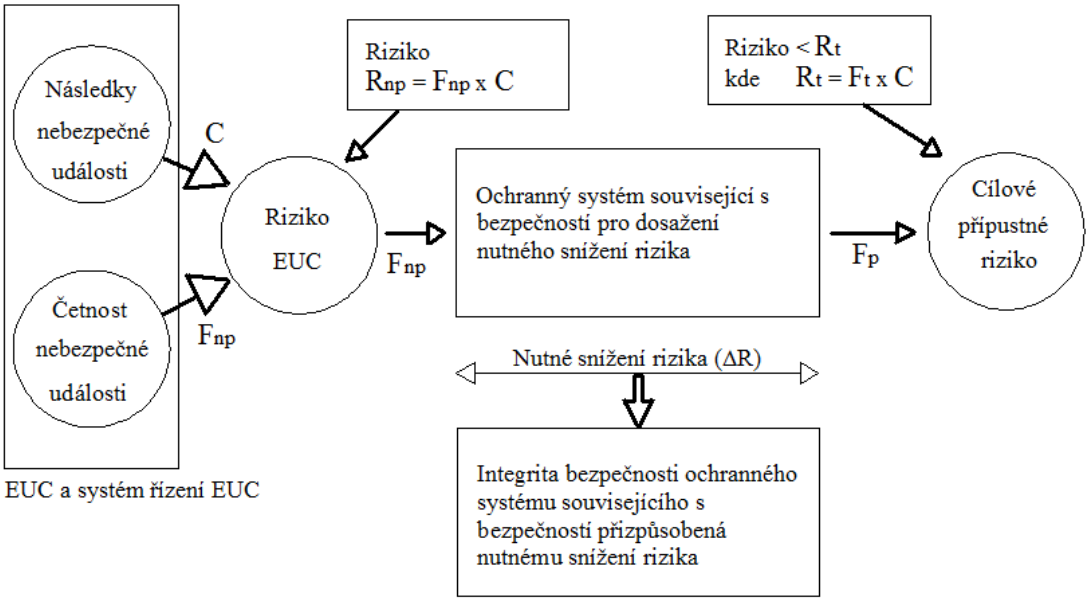
F_t – četnost přípustného rizika,

F_{np} – četnost, s níž by se mohla nebezpečná událost vyskytovat bez použití jakýchkoliv ochranných prostředků,

C – následek nebezpečné události,

F_p – četnosti rizika za přítomnosti ochranných prostředků,

ΔR – nutné snížení rizika. [2]



[2]

Obr. 3 – Příklad ochranného systému souvisejícího s bezpečností

Platí:

$$PFD_{avg} \leq F_t / F_{np} \text{ [-]} \qquad [2]$$

Z důvodu schopnosti určit úroveň integrity bezpečnosti je nutné stanovit F_{np} pro EUC. Vyplývá to především ze vztahu F_{np} k PFD_{avg}. F_{np} stanovíme pomocí:

- analýzy intenzity poruch srovnatelných situací,
- na základě konkrétních dat.

Pomocí pravděpodobnosti PFD_{avg} jsme schopni pomocí tabulky č.1 určit úroveň integrity bezpečnosti SIL (např. pro $PFD_{avg} = 10^{-2}$ až 10^{-3} je úroveň integrity bezpečnosti = 2).

Avšak než se dostaneme k určení SIL musíme dodržet následující kroky:

- určení četnosti rizika bez přidání jakýchkoliv ochranných prostředků,
- určení následku C bez přidání jakýchkoliv ochranných prostředků,
- pomocí tabulky č.7 určíme zda se při F_{np} a následku C dosáhne přípustného rizika, pokud je výsledkem třída I, potom jen nutné další snížení rizika, třídy IV a III jsou považovány za přípustná rizika,
- určení pravděpodobnosti poruchy při vyžádání systému souvisejícího s bezpečností, který plní nutné snížení rizika – při konstantním následku $PFD_{avg} = \Delta R$

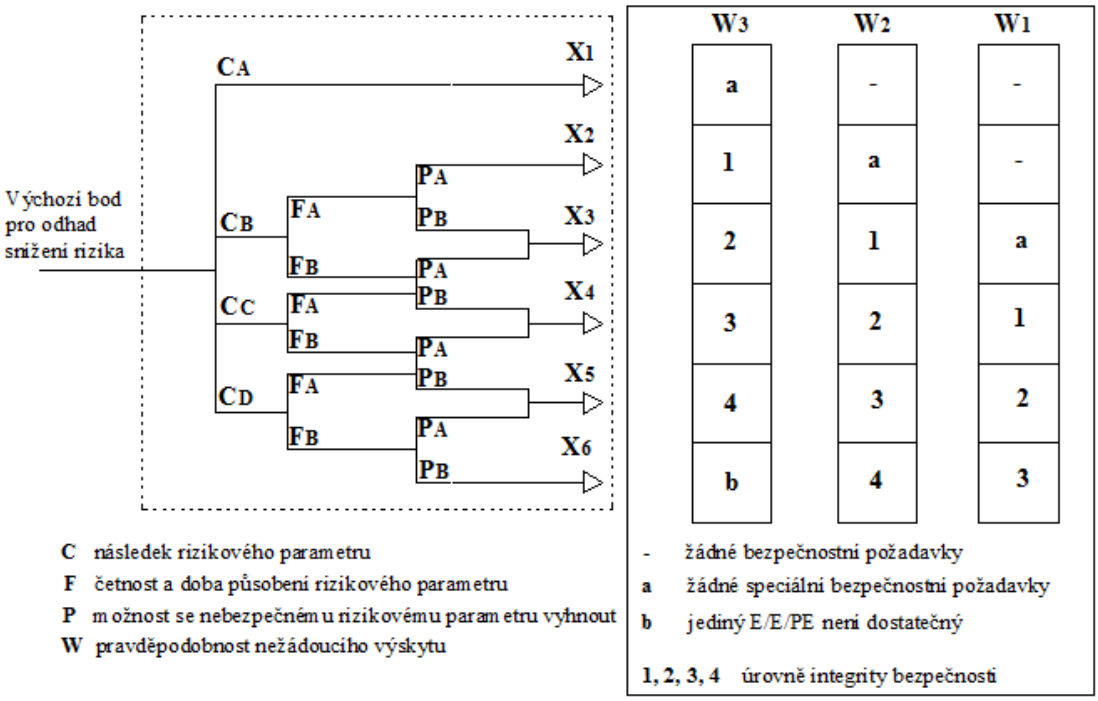
Toto platí, když je následek C konstantní a pokud se nutného dosažení rizika dosahuje jediným systémem souvisejícím s bezpečností, který musí snížit četnost minimálně z F_{np} na F_t. [2]

2.6.2 Metoda diagramu rizika

Metoda diagramu rizika je kvalitativní metoda sloužící pro určení úrovně integrity bezpečnosti systémů souvisejících s bezpečností. Při přijetí kvalitativní metody je nejdříve nutné zavést několik parametrů, které charakterizují základní vlastnosti nebezpečné situace v případě selhání nebo nedostupnosti systému souvisejícího s bezpečností. Tyto parametry jsou:

- následek nebezpečné události (**C**),
- výskyt a doba vystavení v nebezpečné oblasti (**F**),
- možnost se nebezpečné události vyhnout (**P**),
- pravděpodobnost nežádoucího výskytu (**W**).

Jednotlivé parametry je nutné klasifikovat (viz. tabulka č.8) a dále se parametry vzájemně kombinují, aby bylo možné rozhodnout o tom, jakou úroveň integrity přiřadíme systémům souvisejících s bezpečností (viz. obrázek č.4). Dále platí, že čím je úroveň integrity bezpečnosti vyšší, tím účinněji dochází ke snížení rizika. [2]



[2]

Obr. 4 – Diagram rizika (obecné schéma)

Tabulka č.8 – Údaje potřebné pro sestavení diagramu rizika [2]

Rizikový parametr		Klasifikace	Poznámky
Následek nebezpečné událost (C)	C_1 C_2 C_3 C_4	Menší zranění Zranění jedné nebo více osob s trvalými následky nebo smrt jedné osoby Smrt několika osob Smrt velkého počtu osob	Musíme brát v úvahu následky nehod a jejich vyléčení.
Výskyt a doba vystavení nebezpečné události (F)	F_1 F_2	Vzácné až častější vystavení v nebezpečné oblasti Časté až trvalé vystavení v nebezpečné oblasti	Tento parametr bere v úvahu četnost a dobu, po kterou jsou osoby vystaveny nebezpečí.
Možnost se nebezpečné události vyhnout (P)	P_1 P_2	Možné za určitých podmínek Téměř nemožné	Tento parametr zohledňuje: - provoz procesu (s dozorem nebo bez dozoru) - rychlost vzniku nebezpečné události - snadnost rozpoznání nebezpečí - vyhnutí se nebezpečné události,
Pravděpodobnost nežádoucího výskytu (W)	W_1 W_2 W_3	Velmi malá pravděpodobnost – pouze několik nežádoucích výskytů Malá pravděpodobnost – málo nežádoucích výskytů Vysoká pravděpodobnost – časté nežádoucí výskyty.	Účelem činitele W je odhad četnosti nežádoucího výskytu, a to bez přidání systému souvisejících s bezpečností a také bez všech vnějších prostředků pro snížení rizika.

Použití parametrů rizika C, F a P vede na několik mezilehlých výstupů X_1,…..X_n (počet výstupů závisí na konkrétní oblasti, na kterou má diagram rizika platit). Každý z výstupů je mapován do jedné ze tří stupnic (W_1, W_2, W_3). Jednotlivé stupně na těchto stupnicích označují nutnou integritu bezpečnosti, kterou musí systém související s bezpečností splňovat.

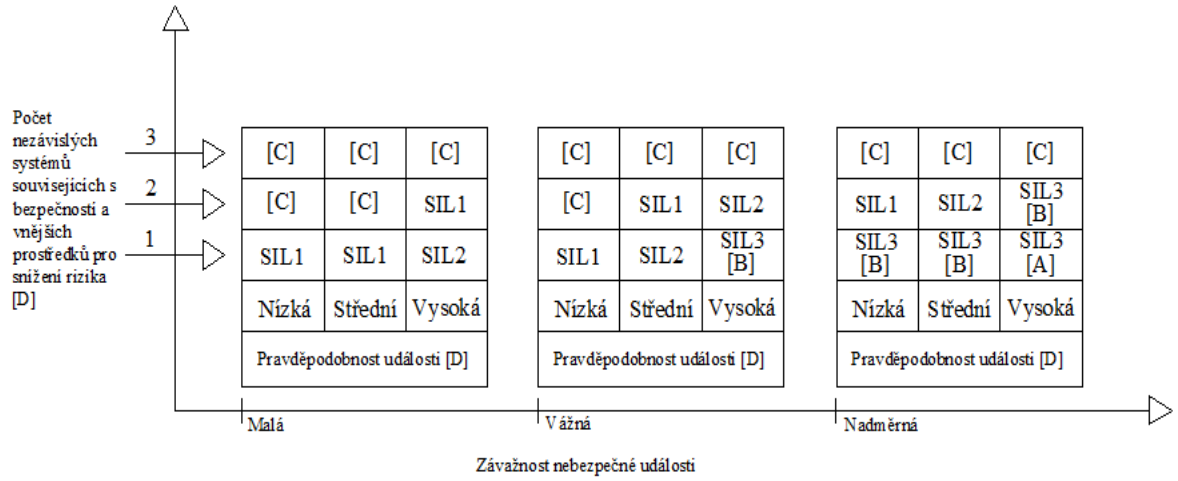
Stupnice W_1 poskytuje maximální přínos (= nejmenší pravděpodobnost nežádoucího výskytu), stupnice W_2 poskytuje střední přínos a stupnice W_3 poskytuje minimální snížení rizika(= největší pravděpodobnost nežádoucího výskytu). Mezilehlé výstupy a konkrétní stupnice W představují výstup diagramu rizika. Tento výstup udává úroveň integrity bezpečnosti systému souvisejícího s bezpečností a představuje míru požadovaného snížení. Toto snížení rizika spolu s dalšími sníženími získaných od jiných opatření, představuje nutné snížení rizika pro danou situaci. [2]

2.6.3 Metoda matice závažnosti nebezpečných událostí

Metoda matice závažnosti je kvalitativní metoda, která slouží k určení úrovně integrity bezpečnosti systému souvisejícího s bezpečností. U této metody se předpokládá, že každý systém související s bezpečností a všechny vnější prostředky pro snížení rizika, jsou na sobě nezávislé.

Konstrukce matice závažnosti je závislá na následujících požadavcích:

a) systémy související s bezpečností a vnější prostředky určené pro snížení rizika jsou nezávislé,
b) systémy související s bezpečností a vnější prostředky pro snížení rizika tvoří tzv. ochranné vrstvy, které poskytují vlastní dílčí snížení rizika,
c) přidáním jedné ochranné vrstvy se zvýší integrita bezpečnosti o jeden stupeň,
d) je použit pouze jeden systém související s bezpečností, u kterého je zjišťována touto metodou úroveň integrity bezpečnosti. [2]



[2]

Obr. 5 – Příklad výsledné matice závažnosti

Vysvětlivky k obrázku č.5:

[A] Použití jednoho systému souvisejícího s bezpečností s SIL 3, nám nezajistí dostatečné snížení úrovně rizika. Jsou proto nutná další přídavná opatření pro snížení rizika.

[B] Použití jednoho systému souvisejícího s bezpečností s SIL 3, nám nezajistí dostatečné snížení úrovně rizika. Jsou nutná další přídavná opatření pro snížení rizika, u kterých se požaduje provedení analýzy nebezpečí a rizik.

[C] Není pravděpodobně požadováno použití nezávislého systému souvisejícího s bezpečností.

[D] Pravděpodobnost události je pravděpodobnost, že k nebezpečné události dojde bez použití jakéhokoliv systému souvisejícího s bezpečností nebo vnějších prostředků pro snížení rizika. [2]

3 Nezávislá topení Eberspächer

Nezávislá topení jsou určena pro vytápění vozidel i při vypnutém motoru. Nezávislá topení se rozdělují na teplovodní topení a teplovzdušná topení. V rámci této práce se budu, z důvodu vybraného typu topení, zabývat pouze topením teplovodním. [5]

3.1 Představení společnosti Eberspächer

Firma Eberspächer působí v České republice od roku 1992. Je součástí německého koncernu Eberspächer. Firma je organizačně rozdělena do dvou samostatných subjektů:
Eberspächer spol. s.r.o. pro oblast výfukové techniky:

- závod na výrobu výfukových systémů sídlí v Rakovníku
- předmětem činnosti je výroba tlumičů a katalyzátorů
- výrobky z tohoto závodu jsou určené pro všechny přední světové výrobce automobilového průmyslu,

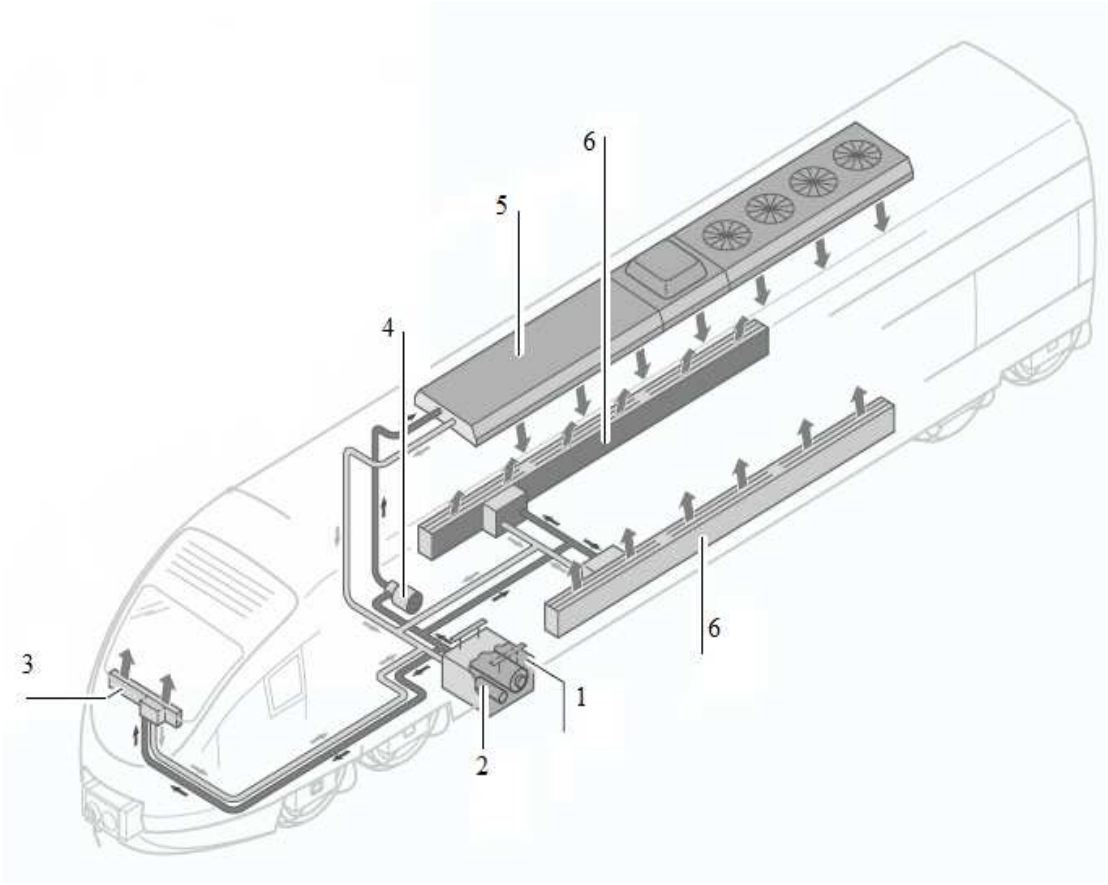
Eberspächer Praha s.r.o. pro oblast nezávislých topení:

- společnost se nachází v Praze 4
- zabývá se prodejem nezávislých topení a ochlazovací techniky. [5]

3.2 Teplovodní topení HYDRONIC

Teplovodní topení pracují nezávisle na motoru. Jsou využívány pro předehřev interiéru, motoru a v létě také pro nezávislé větrání. Topné přístroje jsou integrovány do oběhu chladící kapaliny motoru. Tepelná energie je rozváděna jako teplý vzduch přes vzduchové kanály interiéru. Zbytkovým teplem v chladící kapalině se ohřeje motor. To má vliv na menší opotřebení motoru, zejména v zimních měsících. [5]

3.2.1 Umístění teplovodního topení na kolejovém vozidle



[4]

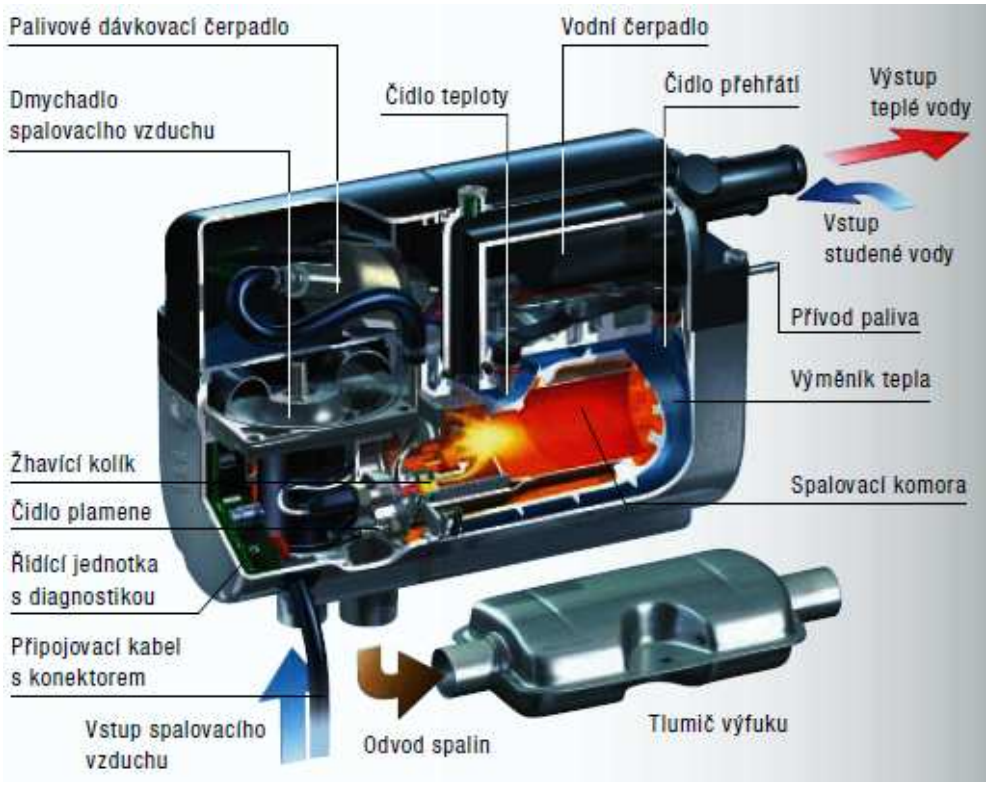
Obr.6 – Instalace teplovodního topení na kolejovém vozidle

Popis součástí na obrázku č.6:

1. Topný přístroj
2. Vodní čerpadlo
3. Přední topné těleso
4. Doplňkové vodní čerpadlo
5. Střešní topení
6. Podlahové topení [4]

U kolejových vozidel se topný přístroj umísťuje pod podlahu vozu do instalační skříně.

3.2.2 Popis součástí a funkce teplovodního topení



[5]

Obr. 7 – části teplovodního topení typu HYDRONIC

Popis funkce teplovodního topení:

Po spuštění topení řídící jednotka provede následující procesy:

a) automatická bezpečnostní kontrola komponentů,
b) spuštění vodního čerpadla,
c) při teplotě topného média < 5°C proběhne předehřev trysky,
d) spuštění hořáku,
e) elektromotor se spustí a pohání palivové čerpadlo a dmychadlo spalovacího vzduchu,
f) zapnutí zapalování, otevření magnetického ventilu a kontrola otáček elektromotoru,
g) vytvoření hořlavé směsi paliva a spalovacího vzduchu,
h) zapálení směsi zapalovací jiskrou pomocí generátoru zapalovací jiskry,
i) čidlo plamene rozpozná frekvenci kolísání plamene a vypne generátor zapalovací jiskry,
j) vzniklé teplo je předáváno výměníkem tepla topnému médiu,
k) teplota topného média je neustále kontrolována čidly teploty a přehřátí,
l) po skončení vytápění se uzavře magnetický ventil a začíná doběh, po jehož skončení dojde k vypnutí přístroje. [4]

3.2.3 Technický popis teplovodního topení typu HYDRONIC L35

Tabulka č.9 – Technické údaje teplovodního topení typu HYDRONIC L35 [4]

Typ topného přístroje	**Hydronic L-II**	
Topný přístroj	**Hydronic L35**	
Provedení	HL2-35	
Topné médium	Směs vody a chladiva (min. 10%, max. 50% chladiva jako ochrana před zamrznutím)	
Tepelný proud [W] (při teplotě prostředí –10°C)	35 000 W	
Hodnoty teploty – na vstupu vody	Vstupní 73°C / Výstupní 78°C	
Hodnoty teploty – na výstupu vody	Vstupní 85°C / Výstupní 118°C	
Palivo	Motorová nafta – standardní (DIN EN 590) Topný olej EL (DIN 51603)	
Spotřeba paliva (při teplotě prostředí – 10°C)	4,2 l/h	
Jmenovité napětí	24 V	
Provozní rozsah: Dolní napěťová hranice: Podpěťová ochrana zabudovaná v řídící jednotce vypne topný přístroj po dosažení napěťové hranice.	20 V	
Provozní rozsah: Horní napěťová hranice: Přepěťová ochrana zabudovaná v řídící jednotce vypne topný přístroj po dosažení napěťové hranice.	30 V	
Připojený příkon (při provozu)	120 W	
Objem vody (v topném přístroji)	cca 2,4 l	
Minimální průtok	3 l/h	
Přípustná teplota prostředí: Topný přístroj Řídící jednotka	V provozu - 40°C až + 85°C - 40°C až + 80°C	Mimo provoz - 40°C až + 100°C - 40°C až + 100°C
Provozní tlak (v topném přístroji)	2,5 bar	
Hodnoty CO_2 (obj. %)	9,5 – 11,5	
Rozměry [mm]	600 / 230 / 220	
CO ve výfukovém plynu	< 0,04	
Hmotnost	cca 18 kg	
Druh ochrany	IP 64	

3.2.4 Technický popis vodního čerpadla typu FLOWTRONIC 6000SC

Technický popis vodního čerpadla je uveden proto, že vodní čerpadlo nebývá zpravidla dodáváno jako vlastní součást teplovodního topení. Při koupi topení je tedy nutné vodní čerpadlo zakoupit zvlášť.

Tabulka č.10 – Technické údaje vodního čerpadla FLOWTRONIC 6000SC [4]

Typ čerpadla	**FLOWTRONIC 6000SC**
Topné médium	Směs vody a chladiva (min. 10%, max. 50% chladiva jako ochrana před zamrznutím)
Přepravované množství	6000 l/h při dopravním tlaku 0,4 bar
Provozní tlak (oběh vody)	Max. 2 bar
Hmotnost	2,5 kg
Jmenovité napětí	24 V
Provozní rozsah	18 – 32 V
Příkon (při průtoku 6000 l/h a dopravním tlaku 0,4 bar)	210 W
Druh ochrany	IP 25
Teplotní podmínky:	
Topné médium	-40°C až +90°C krátkodobě (15min) +115°C
Prostředí, provoz	-40°C až +90°C krátkodobě (30min) +100°C

3.3 Spínací hodiny typu EasyStart T

Tabulka č.11 – Technické údaje spínacích hodin typu EasyStart T [3]

Typ	**EasyStart T**
Provozní napětí	12 V / 24 V
Rozměry	36 x 51 x 10,5 mm
Provozní teplota	- 40°C až + 80°C
Displej LCD	zaručená čitelnost údajů od – 20°C do + 60°C

4 Analýza rizik teplovodního topení – metodika řešení

Pro zpřehlednění postupu řešení je v této kapitole uvedena analýza FMEA a diagram rizika pouze pro jeden komponent teplovodního topení, a to konkrétně pro čidlo plamene. Kompletní analýza FMEA je uvedena v příloze práce.

4.1 Analýza FMEA

Jedná se o první krok řešení práce. Tato metoda byla vybrána, protože k řešení problému nebyly k dispozici konkrétní data o četnosti poruch z provozu. Proto bylo nutné práci řešit kvalitativně, což nám tato metoda umožňuje.

Pro hodnocení příčin a následků poruch pomocí této metody bylo nejdříve nutné rozdělit závažnosti, četnosti a odhalitelnosti poruch do jednotlivých tříd. Každá z těchto tříd byla popsána pomocí číselného a slovního vyjádření. U každé z tříd je také uvedeno vysvětlení, co jaký stupeň představuje. Jednotlivé třídy jsou uvedeny a popsány v tabulkách č.12, 13 a 14. Stupeň s číslem 10 představuje nejhorší důsledek poruchy, největší četnost poruchy a nejhorší odhalitelnost poruchy, stupeň číslo 1 naopak. Počet stupňů a vysvětlení k nim není závazný a přesně určený, záleží na konkrétní oblasti řešení a také na vlastním řešiteli.

Tabulka č.12 – Kritéria určení stupně závažnosti poruchy pro analýzu FMEA

1	**Žádný důsledek**	Systém zůstává v provozuschopném a bezpečném stavu.
2	**Minimální důsledek**	Porucha způsobí vypnutí zařízení, které můžeme po určité době opět zapnout.
3	**Nepatrný důsledek**	Oprava části zařízení, která neovlivňuje provoz ani bezpečnost.
4	**Malý důsledek**	Oprava části, která není součástí zařízení, ale je nezbytná k provozu zařízení a neohrožuje bezpečnost.
5	**Mírný důsledek**	Oprava části zařízení, které nevykonává svoji funkci.
6	**Větší důsledek**	Oprava části zařízení, které vykonává svoji funkci jinak než by mělo.
7	**Významný důsledek**	Oprava části zařízení, která neumožňuje provoz a ohrožuje bezpečnost.
8	**Velký důsledek**	Ohrožení života lidí – odpojením lze zabránit nebezpečí.
9	**Nebezpečný důsledek**	Ohrožení života lidí.
10	**Kritický důsledek**	Ohrožení života lidí – nečekaná událost.

Tabulka č.13 – Kritéria určení stupně četnosti poruch pro analýzu FMEA

1	**Vzácná**	Elektronika nebo součást ze SIL 2
2	**Velice slabá**	Elektronika – umístěna ve špinavém prostředí nebo součást ze SIL 1
3	**Slabá**	Elektronika – vystavena působení vibrací
4	**Nízká**	Elektronika – teplotně namáhaná
5	**Střední**	Elektronika – vystavena min. dvěma výše popsaným vlivům
6	**Mírná**	Mechanické části
7	**Větší**	Mechanické části – umístěny ve špinavém prostředí
8	**Častá**	Mechanické části – vystaveny působení vibrací
9	**Vysoká**	Mechanické části – teplotně namáhané
10	**Velmi vysoká**	Mechanické části – vystaveny min. dvěma výše popsaným vlivům

Při určování četnosti jednotlivých poruch bylo vycházeno z poznatků, že elektronické části mají menší četnost poruch než části mechanické. Podrobnější rozdělení bylo provedeno podle toho v jakém prostředí jednotlivé části pracují a také podle toho zda jsou k určitému komponentu přiřazeny hodnoty SIL, což má význam především u opakované analýze FMEA.

Tabulka č.14 – Kritéria určení odhalitelnosti poruchy pro analýzu FMEA

1	**Jistá**	Okamžitě viditelná (zařízení je nefunkční).
2	**Velmi vysoká**	Snadno rozpoznatelná (př. zařízení vykonává funkci, i když je vypnuto).
3	**Vysoká**	Poruchu zaznamená jiné zařízení přístroje.
4	**Středně vysoká**	Poruchu lze zaznamenat na jiném zařízení vozidla.
5	**Střední**	Nezkušený zákazník rozpozná poruchu.
6	**Malá**	Méně zkušený zákazník rozpozná poruchu.
7	**Velmi malá**	Průměrný zákazník je schopen rozpoznat poruchu.
8	**Slabá**	Zkušenější zákazník je schopen rozpoznat poruchu.
9	**Téměř nemožná**	Poruchu jsme v některých případech schopni odhalit (př. kouř, požár).
10	**Absolutně nemožná**	Není žádná šance odhalení poruchy (př. výbuch).

Kritéria odhalitelnosti poruchy byla volena podle toho, jakým způsobem je obsluha zařízení schopna rozpoznat vznikající poruchu a případně jí zabránit, nebo zda poruchu jsou schopny zaznamenat jiné komponenty teplovodního topení.

4.1.1 Analýza FMEA pro čidlo plamene teplovodního topení

Čidlo plamene má v teplovodním topení funkce:

- po zapálení topného přístroje rozpozná frekvenci kolísání plamene a tím dá impuls řídící jednotce pro vypnutí generátoru zapalovací jiskry, kterým byla hořlavá směs zapálena,
- hlídá vznikající plamen - v případě nevznikajícího plamene, nebo dojde-li po dobu 2 sekund k přerušení plamene, čidlo plamene dá impuls k odregulování,
- jestliže po vypnutí přístroje rozpozná plamen, dojde k vypnutí přístroje.

V zásadě mohou nastat dva stavy poruchy čidla:

- **ztráta funkce** – čidlo nerozpozná vznikající plamen,
- **chyba funkce** – čidlo hlásí přítomnost plamene, i když nevzniká.

Tabulka č.15 – Analýza FMEA pro čidlo plamene

č.	Funkce	Příčina poruchy	Následek	Závažnost	Četnost	Odhalitelnost	RPN
5	Snímání plamene pomocí čidla plamene	Porucha čidla plamene (ztráta funkce)	Nemožnost rozpoznání plamene => nedojde k vypnutí generátoru zapalovací jiskry => poruchu zaznamená řídící jednotka	6	5	3	90
		Porucha čidla plamene (ztráta funkce)	Nerozpozná plamen při doběhu přístroje => v krajním případě může způsobit požár.	9	5	2	90
		Porucha čidla plamene (chyba funkce)	Hlásí přítomnost plamene, když nevzniká => neustálé dodávání paliva do spalovací komory => v krajním případě hrozí výbuch.	10	5	8	400

Ukázka výpočtu RPN (pro chybu funkce čidla plamene):

RPN = závažnost * četnost * odhalitelnost = 10 * 5 * 8 = **400 [-]**

Po přiřazení jednotlivých stupňů ke každému možnému následku poruchy byla vypočítána hodnota významnosti rizika RPN. Avšak do matice závažnosti, která je dalším krokem analýzy FMEA, zaneseme pouze poruchu s největším RPN, tedy následek poruchy by byl nejzávažnější. V tomto případě má nejvyšší hodnotu RPN chyba funkce čidla plamene, konkrétně RPN = 400.

4.1.2 Matice závažnosti (čidlo plamene)

Dalším krokem analýzy FMEA bylo zanesení poruch jednotlivých komponentů do matice závažnosti (kritičnosti). Matice závažnosti je závislost hodnoty RPN na závažnosti poruchy. Je rozdělena do tří polí, které jsou barevně odlišeny.

Hodnoty závažnosti byly dále rozděleny na skupiny, a pro zanesení dané poruchy do určité skupiny bylo vycházeno ze stupňů při hodnocení závažnosti poruchy v rámci analýzy FMEA. Do matice je u každého komponentu zanesena pouze porucha s největším RPN, tedy nejzávažnější. Pomocí barevného odlišení polí matice závažnosti bylo ihned jasné, pro které poruchy bude muset být provedeno snížení rizika. V tomto případě jsou pole označena červenou, žlutou a zelenou barvou. Pro poruchy v červeném poli bylo nutné snížení rizika, pro poruchy v žlutém poli bylo možné snížení rizika a pro poruchy v zeleném poli nebylo nutné žádné snížení rizika. Velikosti a hranice pro jednotlivá pole nejsou přesně stanoveny, při sestavování matice závisí na oblasti aplikace a také na samotném řešiteli. Zpravidla však platí, že pro poruchy v oblasti katastrofické závažnosti je snížení rizika nezbytně nutné.

Na obrázku č.8 je uvedena výsledná matice závažnosti teplovodního topení. Při analýze FMEA bylo dospěno k tomu, že jediná funkce jejíž selhání by ohrozilo život lidí je chyba funkce čidla plamene. Pro tuto funkci je tedy nezbytně nutné provést snížení rizika. Ostatní možné poruchy jsou pouze provozního charakteru. Tyto provozní poruchy způsobí nefunkčnost zařízení což bude mít za následek určité ekonomické ztráty.

Hodnota významnosti rizika **RPN** (Risk Priority Number) [-]	Závažnost poruchy [-]				
	nevýznamná 1,2	nezávažná 3,4	závažná 5,6	kritická 7,8	katastrofická 9,10
500					
400					Čidlo plamene (chyba funkce)
300			Elektromotor (chyba funkce)		
200			Netěsnost tepelného výměníku Magnetický ventil (chyba funkce) Dmychadlo (ztráta funkce) Palivové čerpadlo (ztráta funkce) Vodní čerpadlo (chyba funkce)		
100	Překročení horní napěťové hranice Překročení dolní napěťové hranice	Nefunkčnost zdroje elektrické energie Netěsnost přívodního vedení chladící kapaliny Poškození ochranné mřížky přívodu vzduchu	Čidlo teploty (chyba funkce) Zanesený palivový filtr Čidlo přehřívání (chyba funkce) Generátor zapalovací jiskry (chyba funkce)		
0					

bez opatření
možné opatření
nutné opatření

Obr. 8 – Matice závažnosti pro teplovodní topení

4.1.3 Diagram rizika

Pomocí diagramu rizika můžeme určit jakou úroveň integrity bezpečnosti SIL bude nutné čidlu plamene přiřadit. Diagram rizika uvádí jako jednu z metod pro určení úrovně integrity bezpečnosti norma ČSN EN 61508. Tato metoda byla vybrána konkrétně proto, že umožňuje řešit úlohu kvalitativním způsobem, což bylo v tomto případě nutností. Pro diagram rizika je nutná klasifikace parametrů, které představují základní vlastnosti nebezpečné situace v případě selhání. Klasifikace parametrů byla prováděna pomocí tabulky č.8 uvedené v kapitole 2.6.2.

Vypracovaný diagram rizika pro čidlo plamene:

Tabulka č.16 – Stanovení parametrů potřebných pro diagram rizika

Funkce	Kontrola vznikajícího plamene pomocí čidla plamene.	
Příčina poruchy	Čidlo hlásí přítomnost plamene, i když nevzniká (chyba funkce).	
Následek (C)	**C3**	Pokud čidlo hlásí přítomnost plamene, který nevzniká, do přístroje je neustále dodáváno palivo, což může v krajním případě způsobit výbuch => smrt několika osob.
Režim vyžádání (F)	**F2**	Kontrola plamene je trvalou funkcí přístroje.
Možnost vyhnutí se nebezpečné události (P)	**P2**	Tuto poruchu je téměř nemožné zjistit.
Pravděpodobnost výskytu (W)	**W1**	Velmi malá pravděpodobnost, protože se jedná o elektronickou součást.

1) Postup klasifikace parametrů:

Následek (C):

- chyba funkce čidla plamene způsobí to, že čidlo udává řídící jednotce nesprávnou informaci o vzniku plamene, tedy dává informaci o vznikajícím plameni, který ovšem nevzniká,
- na základě této informace je do spalovací komory neustále dodáváno palivo pro spalování, které nemá jak shořet,
- dochází tedy k neustálému plnění palivem, což může v krajním případě způsobit výbuch,
- tento důsledek poruchy by mohl způsobit smrt až několika osob, což je dle klasifikace parametrů v normě ČSN EN 61508 parametr **C3**.

Režim vyžádání (F):

- tento parametr zohledňuje s jakou četností je daný komponent využíván,
- při chodu topení je vznikající plamen nutno neustále snímat, což znamená, že čidlo plamene je téměř neustále v provozu => četnost vyžádání této funkce je velmi vysoká,
- pro tento způsob vyžádání byl dle tabulky klasifikace parametrů vybrán parametr **F2**.

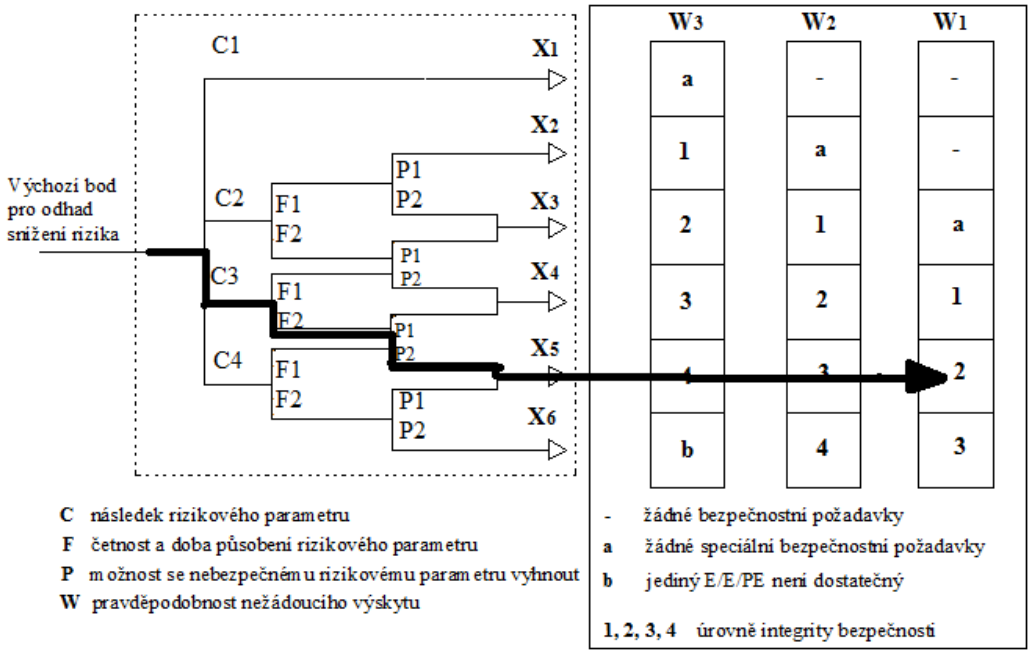
Možnost vyhnutí se nebezpečné události (P):

- v případě chyby funkce čidla plamene není schopna řídící jednotka poruchu rozpoznat,
- poruchu by však mohla zjistit zkušená obsluha, která by včasným zásahem mohla zařízení sama vypnout, porucha by byla rozeznatelná na základě mírného poklesu intenzity teplého vzduchu,
- i přes tento důvod byl tento parametr klasifikován jako **P2**.

Pravděpodobnost výskytu (W):

- při klasifikaci tohoto parametru bylo vycházeno z toho, zda se jedná o mechanickou součást nebo o elektronickou součást,
- čidlo plamene je součást elektronická, tedy pravděpodobnost poruchy tohoto komponentu je velmi malá,
- z tohoto důvodu byl tento parametr klasifikován jako **W1**.

2) Kombinace parametrů = > určení SIL

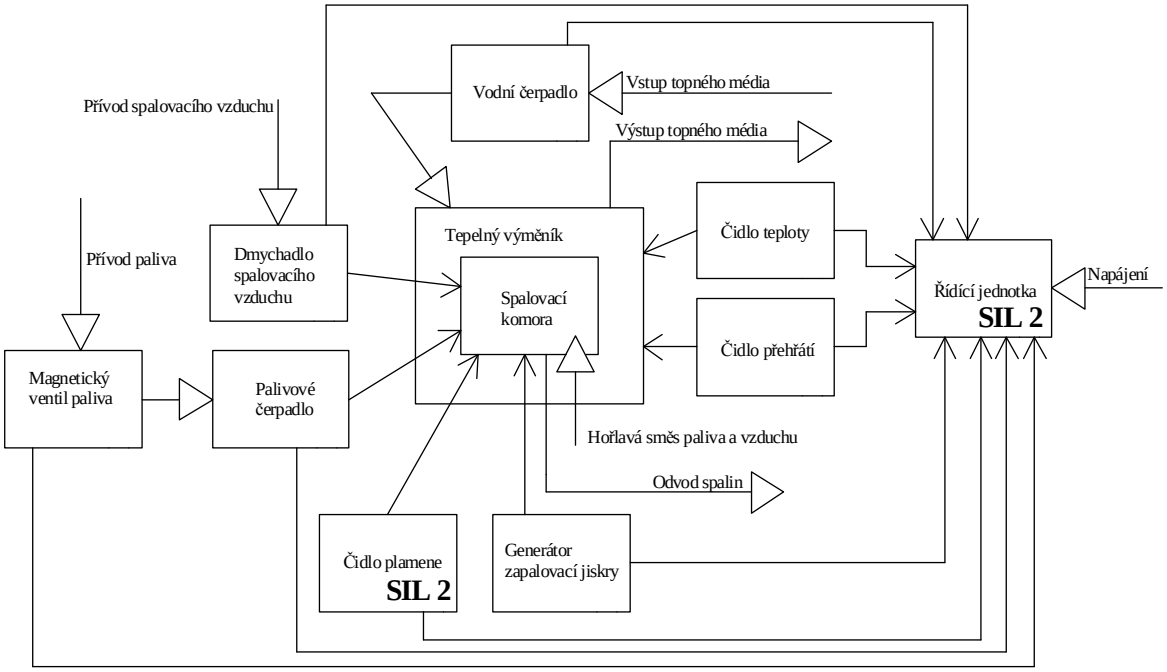


[2]

Obr. 9 – Diagram rizika pro čidlo plamene

Úroveň integrity bezpečnosti pro čidlo plamene **SIL = 2.** To znamená, že čidlu plamene je nutné přiřadit zabezpečovací funkci. Stupeň SIL 2 označuje, že pravděpodobnost nebezpečných poruch musí být v rozsahu **10^{-6} až 10^{-7} poruch za hodinu**.

4.1.4 Určení SIL pro řídící jednotku



Obr. 10 – Součásti teplovodního topení (určení SIL řídící jednotky)

Hodnotu úrovně integrity bezpečnosti SIL pro řídící jednotku určíme pomocí hodnot SIL ostatních součástí zařízení, jejichž funkci řídící jednotka ovládá. Tuto hodnotu určíme tak, že vybereme nejvyšší hodnotu SIL, která byla přiřazena některé z částí.

Pro zpřehlednění a jistějšímu určení SIL řídící jednotce bylo vhodné si dané teplovodní topení rozkreslit a do jednotlivých bloků, které představují komponenty teplovodního topení, přiřadit hodnotu SIL danému komponentu přiřazenou. V tomto případě nejvyšší hodnotu SIL má čidlo plamene, konkrétně SIL = 2. Z tohoto důvodu musíme také řídící jednotce přiřadit **SIL = 2**.

4.1.5 Opakovaná FMEA pro čidlo plamene

Přiřazením úrovně integrity bezpečnosti SIL, tedy přiřazením zabezpečovací funkce, která nám snížila četnost poruch (neboli pravděpodobnost poruchy), dosáhneme při opakované analýze FMEA snížení hodnoty významnosti rizika RPN. Což bylo cílem naší práce, a také nám umožňuje porovnat hodnoty RPN před a po přijetí určité úrovně zabezpečení. V opakované analýze FMEA nám tedy klesnou stupně četností poruchy na úrovně popsané v tabulce č.13 uvedené v kapitole 5.1.

Tabulka č.17 – Opakovaná analýza FMEA pro čidlo plamene

č.	**Funkce**	**Příčina poruchy**	**Následek**	**Závažnost**	**Četnost**	**Odhalitelnost**	**RPN**
5	Snímání plamene pomocí čidla plamene	Porucha čidla plamene (ztráta funkce)	Nemožnost rozpoznání plamene => nedojde k vypnutí generátoru zapalovací jiskry => po určité době poruchu zaznamená řídící jednotka	5	1	3	15
		Porucha čidla plamene (ztráta funkce)	Nerozpozná plamen při doběhu přístroje => v krajním případě může způsobit požár.	9	1	2	18
		Porucha čidla plamene (chyba funkce)	Hlásí přítomnost plamene, když nevzniká => neustálé dodávání paliva do spalovací komory => v krajním případě hrozí výbuch.	10	1	8	80

Ukázka výpočtu RPN (pro chybu funkce čidla plamene):

RPN = závažnost * četnost * odhalitelnost = 10 * 1 * 8 = **80 [-]** => před zabezpečením hodnota RPN = 400.

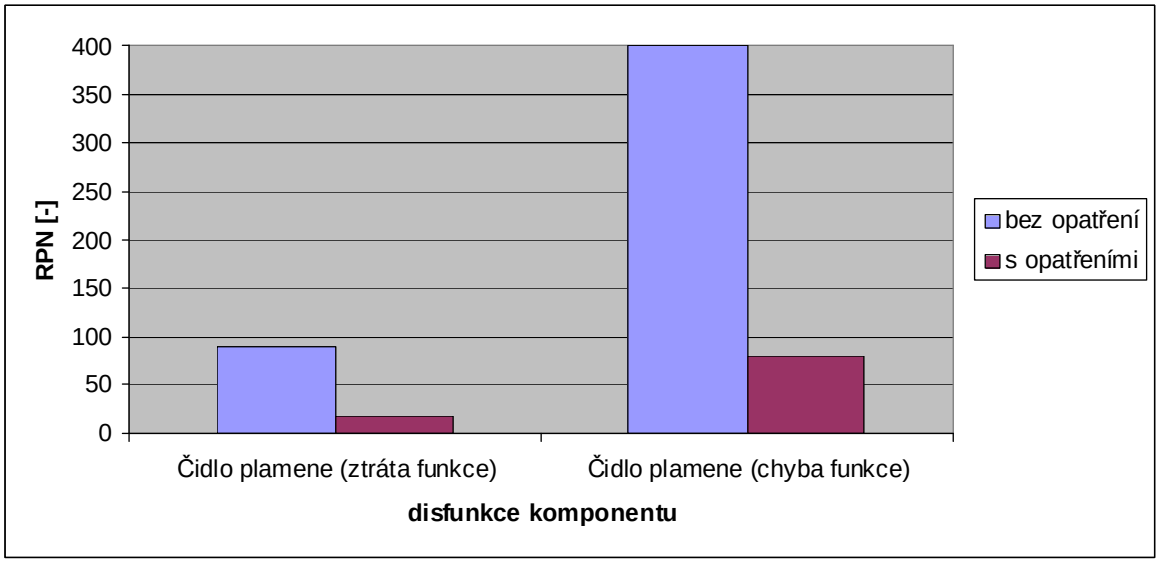
4.2 Posouzení redukce rizika

Redukce rizika poruchy čidla plamene:

Posouzení snížení hodnoty významnosti rizika RPN před a po přijetí bezpečnostních požadavků. Posouzení je provedeno pouze pro poruchy čidla plamene, protože po vypracování analýzy FMEA bylo zjištěno, že možná porucha pouze tohoto komponentu by mohla způsobit ohrožení života lidí. Proto bylo nutné přiřadit úroveň integrity bezpečnosti SIL, tedy zabezpečovací funkci, pouze tomuto komponentu. Jednotlivé poruchy jsou zaneseny grafu na obrázku č.12, který slouží pro grafické znázornění redukce rizika.

Tabulka č.18 – Hodnoty pro graf posouzení redukce rizika

RPN bez opatření [-]	Komponent (způsob poruchy)	RPN s opatřeními [-]
90	Čidlo plamene (ztráta funkce)	18
400	Čidlo plamene (chyba funkce)	80



Obr. 11 – Posouzení redukce rizika

Redukce rizika (čidlo plamene):

- nejzávažnější porucha – chyba funkce
- úroveň integrity bezpečnosti SIL = 2
- hodnota RPN (chyba funkce) – bez opatření RPN = 400, s opatřeními RPN = 80
- hodnota RPN (ztráta funkce) – bez opatření RPN = 90, s opatřeními RPN = 18

=> **redukce rizika = 80 %**

5 Závěr

Funkční bezpečnost klade vysoké nároky na spolehlivost komponentů a tím zabránit ohrožení života lidí, životního prostředí nebo vzniku materiálových ztrát. Pomocí analýzy FMEA jsem stanovil, že chyba funkce pouze u jednoho komponentu teplovodního topení, může způsobit ohrožení života lidí. Konkrétně se jedná o chybu funkce čidla plamene, kdy čidlo hlásí opačnou hodnotu než jakou by mělo. Tato porucha je však v praxi velmi málo pravděpodobná a z hlediska přihlédnutí ke zkušenostem s provozem tohoto přístroje, můžeme říci, že tato porucha je téměř nemožná. Avšak i přes tento důvod bylo nutné snížit riziko vzniku této poruchy tak, že čidlu plamene byla přiřazena hodnota úrovně integrity bezpečnosti SIL. Přiřazením SIL vlastně upozorníme na nutnost zabezpečení tohoto komponentu. Konkrétně pro čidlo plamene byla stanovena úroveň integrity bezpečnosti SIL = 2. Tím pádem by došlo k redukci rizika možnosti vzniku poruchy o 80 %. Snížení rizika by v tomto případě mohlo být považováno za přijatelné, s přihlédnutím na možnost vzniku poruchy před přiřazením úrovně integrity bezpečnosti, tedy bez určitých bezpečnostních opatření.

Jako technicky nespolehlivější úpravu proti vzniku chyby funkce čidla plamene by bylo použití dvou paralelních čidel snímajících plamen. Obě čidla by komunikovala navzájem spolu, ale také s řídící jednotkou. To by vlastně znamenalo, že pokud budou čidla dávat různé informace řídící jednotce dojde k poruchovému vypnutí, čímž bychom vlastně téměř úplně eliminovali možnost vzniku této poruchy.

Ostatní analyzované možnosti poruch byly pouze provozního charakteru, tedy v případě vzniku těchto poruch by byla nutná pouze oprava zařízení, která by zapříčinila určité ekonomické ztráty. Avšak jako cíl práce jsem si určil snížit riziko pro poruchy ohrožující život osob. Z tohoto důvodu jsem těmto poruchám nepřiřadil úrovně integrity bezpečnosti SIL. Přiřazením SIL těmto komponentům by mohlo prodloužit spolehlivost a životnost těchto komponentů, a tedy celého přístroje. Toto by se týkalo výměníku tepla, magnetickému ventilu, dmychadlu, palivovému čerpadlu a vodnímu čerpadlu. To bychom především ocenili s přihlédnutím k nákladům na provoz přístroje. Stanovení úrovně integrity bezpečnosti by tedy způsobilo to, že komponenty by byly spolehlivější, čímž se poměrně výrazně zvýší jejich životnost a sníží možnost jejich selhání. Avšak takováto opatření by zapříčinila zvýšení ceny celého přístroje.

V dnešní době výrobce topení doporučuje výměnu kompletního topení po provozní době 5000 hodin. Toto je doba životnosti zařízení, ve které výrobce zaručuje téměř žádný výskyt poruch. Cena kompletního topení HYDRONIC L35, se všemi díly a se zahrnutím práce, se pohybuje kolem 100 000 Kč. Tyto náklady je tedy nutné vynaložit po uběhnutí doby životnosti zařízení. Po přiřazení bezpečnostních by došlo k prodloužení životnosti výrobku a tím vlastně ke snížení nákladů na jeho provoz.

6 Seznam použité literatury

[1] ČSN EN 60812. *Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA)*. 2007.

[2] ČSN EN 61508. *Funkční bezpečnost elektrických/elektronických/programovatelných systémů souvisejících s bezpečností*. 2002.

[3] EBERSPÄCHER. *EasyStart T Komfortní spínací hodiny s možností předvolby na 7 dnů*. 2005. 45s.

[4] EBERSPÄCHER. *Hydronic L-II Technický popis, návod k instalaci, obsluze a údržbě*. 2008. 43s.

[5] EBERSPÄCHER. *Nezávislá topení Eberspächer, nezávislé klimatizace, nezávislé ochlazovače, Incinerátor WC16 a speciální aplikace topení V7S*. 15s.

[6] FAMFULÍK, Jan; MÍKOVÁ, Jana. Příspěvek k analýze rizika modulu automatického vedení vlaku. *Perner´s Contacts* [online]. Listopad 2009 [cit. 2.ledna 2010]. Dostupný na WWW: <http://pernerscontacts.upce.cz/15_2009/Famfulik2.pdf >. ISSN 1801-674X.

7 Seznam tabulek a obrázků

Příloha A

Kompletní analýza FMEA teplovodního topení

Tabulka č.1 – Analýza FMEA pro funkci č.1

č.	Funkce	Příčina poruchy	Následek	Závažnost	Četnost	Odhalitelnost	RPN
1	Přečerpávání vody pomocí vodního čerpadla	Nefunkčnost čerpadla – např. přerušení cívky relé, zkrat cívky relé (ztráta funkce)	Čerpadlo nevykonává požadovanou funkcí => v topném přístroji dojde k výraznému omezení množství protékající vody => dochází k přehřívání přístroje => porucha zachycena čidlem přehřátí.	5	8	3	120
		Malý výkon čerpadla – např. zanesení nečistotami (chyba funkce)	Nízký průtok => přehřívání přístroje (dochází k nedostatečnému odvádění tepelné energie topným médiem) => porucha zachycena čidlem přehřátí nebo čidlem teploty.	6	8	3	144
		Netěsnost přívodního vedení nebo špatné odvzdušnění okruhu chladící kapaliny	Nízký (popř. žádný) průtok => přehřívání přístroje (dochází k nedostatečnému odvádění tepelné energie topným médiem) => porucha zachycena čidlem přehřátí nebo čidlem teploty.	4	6	3	72

Tabulka č.2 – Analýza FMEA pro funkci č.2

č.	Funkce	Příčina poruchy	Následek	Závažnost	Četnost	Odhalitelnost	RPN
2	Elektromotor pohání dmychadlo spalovacího vzduchu a palivové čerpadlo	Nízký výkon elektromotoru (chyba funkce)	Nízký výkon zařízení. Zařízení není schopno vykonávat požadovanou funkci v plném rozsahu.	6	8	6	288
		Nefunkční elektromotor (ztráta funkce)	Nedochází k plnění vzduchu pro spalování a plnění palivem => nedojde k zapálení => porucha zachycena čidlem plamene.	5	8	3	120
		Poškození (ztráta) ochranné mřížky přívodu spalovacího vzduchu nebo přívodní hadice	Možnost vnesení větších částí do přístroje (v nejhorším případě ucpání přívodního vedení) => nedochází k plnění spalovacím vzduchem => zhasne plamen, nebo přístroj se nezapálí => porucha zachycena čidlem plamene.	4	6	3	72
		Zanesený filtr paliva	Nedostatek přiváděného paliva => přístroj se nezapálí => porucha zaznamenána čidlem plamene.	5	6	3	90
		Nefunkční dmychadlo (ztráta funkce)	Nedochází k plnění vzduchem => přístroj se nezapálí => porucha je zaznamenána čidlem plamene.	5	8	3	120
		Nefunkční palivové čerpadlo – např. poškozená spojka (ztráta funkce)	Nedochází k plnění palivem přístroj se nezapálí => porucha je zaznamenána čidlem plamene.	5	8	3	120

Tabulka č.3 – Analýza FMEA pro funkci č.3, 4, 5

č.	Funkce	Příčina poruchy	Následek	Závažnost	Četnost	Odhalitelnost	RPN
3	Otevření magnetického ventilu	Nefunkčnost ventilu (ztráta funkce)	Nedochází k plnění palivem => nezapálení přístroje => neúspěšný start, překročení bezpečnostní doby => porucha zaznamenána čidlem plamene	5	8	3	120
		Nefunkčnost ventilu (chyba funkce)	Po vypnutí přístroje dochází k neustálému plnění palivem => stálé hoření => pokud do 10 s nezhasne plamen => poruchu zaznamená čidlo plamene => řídící jednotka vypne palivové čerpadlo a dmychadlo	6	8	3	144
4	Zapálení směsi paliva a vzduchu pomocí generátoru zapalovací jiskry	Nefunkční generátor zapalovací jiskry (ztráta funkce)	Nedojde k zapálení přístroje => neúspěšný start, překročení bezpečnostní doby.	5	5	3	75
		Nefunkční generátor zapalovací jiskry (chyba funkce)	Neustále vzniká zapalovací jiskra => poruchu zaznamená řídící jednotka.	6	5	3	90
5	Snímání plamene pomocí čidla plamene	Porucha čidla plamene (ztráta funkce)	Nemožnost rozpoznání plamene => nedojde k vypnutí generátoru zapalovací jiskry => poruchu zaznamená řídící jednotka	5	5	3	75
		Porucha čidla plamene (ztráta funkce)	Nerozpozná plamen při doběhu přístroje => v krajním případě může způsobit požár.	9	5	2	90
		Porucha čidla plamene (chyba funkce)	Hlásí přítomnost plamene, když nevzniká => neustálé dodávání paliva do spalovací komory => v krajním případě hrozí výbuch.	10	5	8	400

Tabulka č.4 – Analýza FMEA pro funkci č.6, 7, 8

č.	**Funkce**	**Příčina poruchy**	**Následek**	**Závažnost**	**Četnost**	**Odhalitelnost**	**RPN**
6	Předávání horkých spalin topnému médiu pomocí tepelného výměníku	Netěsnost v místech svarových spojení tepelného výměníku	Možnost vniknutí chladící kapaliny do spalovací komory => nemožnost hoření => porucha zaznamenána čidlem plamene.	5	10	3	150
7	Kontrola přehřívání pomocí čidla přehřátí	Nefunkční čidlo přehřívání (ztráta funkce)	Dojde k zablokování řídící jednotky, z důvodu, že čidlo nekomunikuje s čidlem teploty.	5	5	3	75
		Nefunkční čidlo přehřívání (chyba funkce)	Čidlo hlásí hodnoty mimo provozní rozsah => velký rozdíl naměřených hodnot čidlem teploty a přehřátí => vypnutí zařízení.	6	5	3	90
8	Regulování teploty topného média pomocí čidla teploty.	Nefunkční čidlo teploty (ztráta funkce)	Dojde k zablokování řídící jednotky, z důvodu, že čidlo nekomunikuje s čidlem přehřátí.	5	5	3	75
		Nefunkční čidlo teploty (chyba funkce)	Čidlo hlásí hodnoty mimo provozní rozsah => velký rozdíl naměřených hodnot čidlem teploty a přehřátí => vypnutí zařízení.	6	5	3	90

Tabulka č.5 – Analýza FMEA pro funkci č.9

č.	Funkce	Příčina poruchy	Následek	Závažnost	Četnost	Odhalitelnost	RPN
9	Napájení topného přístroje elektrickou energií	Překročení horní napěťové hranice	Dochází-li k překročování povolené hranice napájecího napětí po dobu 20 s => porucha je zaznamenána přepěťovou ochranou.	2	3	2	12
		Překročení dolní napěťové hranice	Dochází-li k překročování povolené hranice napájecího napětí po dobu 20 s => porucha je zaznamenána podpěťovou ochranou.	2	3	2	12
		Nefunkčnost zdroje elektrické energie (popř. poškozené přívodní vedení)	Přístroj nemá potřebnou energii pro chod => způsobí nefunkčnost zařízení.	4	3	1	12